

Aws Trusted Secure Enclaves

G-Cloud

January 2026

Table of Contents

1	Service Overview
2	Our Approach
3	Getting Started
4	Your Responsibilities
5	Security & Compliance
6	Support & Exit
7	Why Appvia
8	Contact Us

AWS Trusted Secure Enclaves

Hardened AWS cloud foundation for defence, national security, and sensitive workloads requiring enhanced isolation and stricter security controls aligned with NIST 800-53.

1 Service Overview

Appvia delivers AWS Trusted Secure Enclaves (TSE) for organisations requiring enhanced security controls for classified, sensitive, or mission-critical workloads. Based on AWS TSE-SE architecture with prescriptive security controls.

What you get:

- **TSE-SE reference architecture** — Hardened foundation for sensitive workloads
- **Workload isolation** — Rigorous separation throughout the technology stack
- **NIST 800-53 alignment** — Prescriptive security controls
- **Customer-controlled encryption** — Enhanced key management
- **Cryptographic attestation** — Controlled data channels
- **Strict access governance** — Centralised identity with least privilege
- **Comprehensive logging** — Forensic and compliance requirements
- **Network segmentation** — No external access by default
- **FedRAMP/IRAP alignment** — International security profiles

Expert delivery from DV-cleared secure cloud specialists.

2 Our Approach

We follow a structured approach to deliver hardened secure environments for sensitive workloads.

Implementation phases:

Phase	Activities
-------	------------

Design	Security requirements, control mapping, architecture design
Build	TSE deployment, encryption configuration, policy enforcement
Validate	Security control testing, compliance validation, penetration testing
Handover	Documentation, clearance-appropriate knowledge transfer

Security controls: - Service Control Policies enforcing strict boundaries - Network segmentation preventing unauthorised access - Enhanced encryption with customer-controlled keys - Comprehensive audit logging for security accreditation - Identity governance with strict access controls

Stricter isolation than standard Landing Zone architectures.

3 Getting Started

TSE implementations typically take 8-12 weeks depending on security requirements:

Phase 1: Design Security requirements gathering, NIST 800-53 control mapping, architecture design, and security stakeholder approval.

Phase 2: Build TSE infrastructure deployment, encryption configuration, policy enforcement, and network segmentation.

Phase 3: Validate Security control testing, compliance validation, penetration testing, and accreditation support.

Phase 4: Handover Documentation delivery, cleared personnel knowledge transfer, and operational transition.

Prerequisites: - Security clearance requirements defined - NIST 800-53 or equivalent control baseline identified - AWS Organisation with appropriate administrative access - Cleared personnel for knowledge transfer

Note: This service is for organisations requiring enhanced security controls. Personnel access requires appropriate clearances.

4 Your Responsibilities

To ensure successful service delivery, you will need to:

- Provide timely access to required resources, stakeholders, and information
- Make appropriate subject matter experts available for design and integration discussions
- Ensure business users are available for acceptance testing as agreed
- Procure necessary software licenses and subscriptions
- Empower your project team to make decisions in a timely manner
- Review and approve deliverables based on agreed acceptance criteria
- Define security clearance requirements and control baseline
- Provide AWS Organisation with appropriate administrative access
- Ensure cleared personnel are available for knowledge transfer
- Coordinate with security accreditation authority
- Approve security architecture and control configurations

5 Security & Compliance

This service supports workloads classified up to **Official-Sensitive** where appropriate controls are in place.

Our security credentials:

- **ISO 27001:2013** and **ISO 9001:2015** certified
- **Cyber Essentials Plus** certified
- **75%+ of our team hold SC clearance**
- All access to customer environments is logged and auditable
- Data remains within UK regions unless explicitly agreed

We operate in alignment with GDS, NCSC, and CDDO security principles.

6 Support & Exit

Ongoing Support

- Dedicated Service Delivery Manager as your primary contact
- Regular service reviews with clear reporting on performance and incidents
- Defined change management aligned with ITIL best practices

Knowledge Transfer

We embed knowledge sharing throughout our engagement: - Documented runbooks and operational procedures - Regular knowledge sharing sessions with your team - Post-incident reviews that share learnings

Exit Process

When the engagement ends, we ensure an orderly transition: - Complete documentation of all configurations and procedures - Knowledge transfer sessions as required - 90-day standard notice period - No disruption to your services during handover

7 Why Appvia

We're a UK-based SME with deep expertise in cloud platforms and a strong track record delivering for UK government.

Cloud Partnerships

- AWS Advanced Tier Services Partner & Public Sector Partner
- Microsoft Azure Solutions Partner
- Google Cloud Partner

Open Source Credentials

- Creators of Terranetes (CNCF project for Terraform on Kubernetes)
- Developers of Wayfinder, a self-service cloud platform

Public Sector Experience

We understand the unique requirements of government and public sector organisations, from security clearance to GDS service standards.

"Appvia have helped us realise our cloud-first strategy with excellent product solutions. The security, governance and peace of mind brought in by the cloud landing zone has dramatically accelerated our journey to cloud-native adoption."

— **Peter Macchiocci**, Bank of England, Head of Platform Engineering

8 Contact Us

To discuss your requirements or request a detailed proposal, contact our Public Sector Team.

Phone: 020 3917 2888

Email: sales@appvia.io

Website: www.appvia.io

When you get in touch, please include: 1. The name of this service 2. Your organisation name 3. Your contact details 4. A brief description of your requirements

We'll arrange a discovery call to understand your needs and provide a tailored response.

Appvia helps organisations build, secure, and innovate across cloud, data platforms, and AI by blending practical engineering expertise with real-world experience.



About Appvia

Appvia helps organisations build, secure, and innovate across cloud, data platforms, and AI by blending practical engineering expertise with real-world experience. Drawing on our background in creating open source CNCF projects like Terranetes and our self-service developer platform, Wayfinder, we bring that industry know-how and expertise into your organisation to help unlock the true value of the Cloud. As an AWS Advanced Tier Partner and a Microsoft Solutions Partner, we specialise in delivering secure, scalable cloud-native platforms and services, including containerisation, FinOps, modernisation, and AI integration.

Build, secure, and innovate in the cloud | www.appvia.io



This document contains information that may be privileged or confidential and is the property of Appvia Ltd.

Public Copyright 2026 Appvia Ltd. All rights reserved.